Generalized Galbraith's Test: Characterization and Applications to Anonymous IBE Schemes

Paul Cotan[1,2] and George Teşeleanu[1,3]

[1] Advanced Technologies Institute
10 Dinu Vintilă, Bucharest, Romania
{paul.cotan,tgeorge}@dcti.ro
[2] Department of Computer Science
"Al.I.Cuza" University of Iaşi, Iaşi, Romania
[3] Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania

Abstract. The main approaches currently used to construct identity based encryption (IBE) schemes are based on bilinear mappings, quadratic residues and lattices. Among them, the most attractive approach is the one based on quadratic residues, due to the fact that the underlying security assumption is a well understood hard problem. The first such IBE scheme was constructed by Cocks and some of its deficiencies were addressed in subsequent works. In this paper, we will focus on two constructions that address the anonymity problem inherent in Cocks' scheme and we will tackle some of their incomplete theoretical claims. More precisely, we rigorously study Clear *et. al* and Zhao *et. al*'s schemes and give accurate probabilities of successful decryption and identity detection in the non-anonymized version of the schemes. Also, in the case of Zhao *et. al*'s scheme, we give a proper description of the underlying security assumptions.

Keywords: Galbraith's test, anonymity, identity-based encryption, probability distribution, statistical distance

1 Introduction

From a desire to avoiding several issues[4] inherent to public-key cryptography, Shamir came up in 1984 with an interesting and novel concept: identity based encryption [12]. In the IBE model, a user's public key is simply derived from some of the user's personal data such as his e-mail address, his phone number or even his personal address.

Unfortunately, the construction of a practical IBE scheme was postponed until 2001, when two such schemes where proposed. The first one was proposed by Boneh and Franklin [4] and is based on bilinear maps. Shortly, using a different approach, Cocks proposed a scheme based on quadratic residues [8]. Despite the

[4] *e.g* management of trust, public key recovery

simplicity of his idea, a disadvantage of the scheme is that it has a large ciphertext per plaintext ratio. More precisely, to encrypt one bit we have to transmit two large integers.

As pointed out in [4], Cocks' proposal does not provide anonymity in the sense of Bellare *et al.* [2]. Concretely, Galbraith devised a test that can distinguish which identity was used to create a given Cocks-like ciphertext. The test has been thoroughly analyzed in [1, 13]. Despite this impediment, several schemes that achieve anonymity have been proposed in the literature [1, 5, 7, 9, 11, 15].

In terms of ciphertext expansion, the most efficient anonymous proposal is the one described by Boneh, Gentry and Hamburg [5]. However, encryption time is quartic in the security parameters, and thus makes the scheme very inefficient. Two years later, Ateniese and Gasti [1] propose a practical scheme that achieves anonymity. Moreover, the scheme is universally anonymous (*i.e.* the anonymization process is independent of encryption and requires only access to the user's id). The scheme is further improved by Schipor [11]. By using a trial and error method, he manages to shrink the size of Ateniese and Gasti-type ciphertexts.

A xor-homomorphic variant, that is also universally anonymous, was proposed by Clear *et al.* [6, 7]. By switching to polynomials, they where able to show that scheme has an underlying algebraic structure. This structure was later studied and simplified by Joye [9]. As a consequence, he managed to improve both the speed and ciphertext expansion of Clear *et al.*'s IBE scheme. Using an earlier study [13], Nica and Ţiplea [10] reassess Joye's proposal and provide a simpler description of the scheme. By taking a different approach, Zhao *et al.* [15] manage to further speed-up encryption. Unfortunately, they have twice the ciphertext expansion compared to Joye's scheme.

In this paper we reevaluate some of the claims made by Clear *et al.* [6, 7] and Zhao *et al.* [15] regarding their proposals. More precisely, we rigorously formulate and prove some of the claims made by these authors. Thus, providing the reader with a better understanding of the intrinsic algebraic structures in both schemes.

Structure of the paper. We introduce notations and definitions used throughout the paper in Section 2. The extension of Galbraith's test to polynomial rings is rigorously studied in Section 3. In Sections 4 and 5 we apply our results to obtain precise characterizations of Clear *et al.* and Zhao *et al.* IBE schemes. We conclude with Section 6.

2 Preliminaries

Notations. Throughout the paper, λ denotes a security parameter. Also, the notation $|S|$ denotes the cardinality of a set S. The action of selecting a random element x from a sample space X is denoted by $x \overset{\$}{\leftarrow} X$, while $x \leftarrow y$ represents the assignment of value y to variable x. The probability of the event E to happen is denoted by $Pr[E]$. The quotient of the integer division of a by n, assuming $n \neq 0$, is denoted a div n.

The Jacobi symbol of an integer a modulo an integer n is represented by $J_n(a)$. We let QR_n and QNR_n be the set of quadratic and, respectively, non-quadratic residues modulo n. Also, J_n denotes the sets of integers modulo n with Jacobi symbol 1.

2.1 Identity-based encryption

An IBE scheme consists of four probabilistic polynomial-time (PPT) algorithms, namely *Setup*, *KeyGen*, *Enc* and *Dec*. The input of the first algorithm is the security parameter and the output is the master secret key and system's public parameters. The following algorithm requires as input the set formed by an identity *id*, the master secret key and the public parameters and returns a private key associated to *id*. The third algorithm, *Enc*, receives a message m, an identity *id* together with the public parameters and encrypts m using a key derived from *id* obtaining the ciphertext c. The last algorithm, *Dec*, decrypts c by using the private key associated to *id* and acquiring the initial message m.

Definition 1 (Anonymity and Indistinguishability under Selective Identity and Chosen Plaintext Attacks - ANON-IND-ID-CPA**).** *The* ANON-IND-ID-CPA *security of an IBE scheme $\mathcal{S}$ is formulated by means of the following game between a challenger C and an adversary A:*

Setup(λ): The challenger C generates the public parameters pp and sends them to adversary A, while keeping the master key msk to himself.

Queries: The adversary issues a finite number of adaptive queries. A query can be one of the following types:

- *Private key query. When A requests a query for an identity, the challenger runs the KeyGen algorithm and returns the resulting private key to A.*
- *Encryption query. Adversary A can issue only one query of this type. He sends C two pairs (id_0, m_0) and (id_1, m_1) consisting of two equal length plaintexts m_0 and m_1 and two identities id_0 and id_1. The challenger flips a coin $b \in \{0,1\}$ and encrypts m_b using id_b. The resulting ciphertext c is sent to the adversary. The following restrictions are in place: private key queries for id_0 and id_1 must never be issued.*

Guess: In this phase, the adversary outputs a guess $b' \in \{0,1\}$. He wins the game, if $b' = b$.

The advantage of an adversary A attacking an IBE scheme is defined as

$$\mathrm{IBEAdv}_{A,\mathcal{S}}(\lambda) = |Pr[b = b'] - 1/2|$$

where the probability is computed over the random bits used by C and A. An IBE scheme is ANON-IND-ID-CPA *secure, if for any PPT adversary A the advantage* $\mathrm{IBEAdv}_{A,\mathcal{S}}(\lambda)$ *is negligible. If we consider $id_0 = id_1$ in the above game, we obtain the concept of* IND-ID-CPA *security.*

We further state the security assumption used to prove the security of the IBE schemes mentioned in this paper.

Definition 2 (Quadratic Residuosity - QR). *Choose two large prime numbers $p, q \geq 2^\lambda$ and compute $n = pq$. Let A be a PPT algorithm that returns 1 on input (x, n) if $x \in QR_n$. We define*

$$ADV_A^{\text{QR}}(\lambda) = \left| Pr[A(x,n) = 1 | x \overset{\$}{\leftarrow} QR_n] - Pr[A(x,n) = 1 | x \overset{\$}{\leftarrow} J_n \setminus QR_n] \right| .$$

The Quadratic Residuosity assumption states that for any PPT algorithm A the advantage $ADV_A^{\text{QR}}(\lambda)$ is negligible.

3 Generalized Galbraith's Test

According to [1,3], Galbraith developed a test which shows that Cocks' scheme [8] is not anonymous. A straightforward generalization of Galbraith's test to the ring $\mathbb{Z}_n[x]/(x^2 - R)$ was introduced in [6,7]. More precisely, we define the generalized Galbraith test as

$$GT_n(R, f_0x + f_1) = J_n(f_1^2 - f_0^2R),$$

where $R \in J_n$ and $f_0x + f_1 \in Z_n[x]/(x^2 - R)$.

The authors of [6,7] briefly describe some aspects of the generalized version of the test, but some of their claims were not rigorously formulated and/or proved. More precisely, they assume that $f_0, f_1 \in \mathbb{Z}_n^*$ and this is not always the case[5]. Remark that when $f_0, f_1 \in \mathbb{Z}_n^*$, the generalized Galbraith test is identical to the original Galbraith test.

In this limited scenario, Clear *et al.* prove that their scheme is anonymous by reducing their security proof to some result from [1, 13]. Although is not explicitly mentioned in [6,7], using the results from [1,13] we can also compute the success probability of Galbraith's test when we choose to use Clear *et al.*'s IBE scheme without implementing the anonymization technique.

The generalized Galbraith test is also used in [15] to show that their scheme is not anonymous. Although the authors also assume that $f_0, f_1 \in \mathbb{Z}_n^*$, they do not compute the test's success probability for their IBE scheme and in this case the probability cannot be derived from [1, 13].

Motivated by these applications, we further study the generalized Galbraith test without any restrictions. More precisely, our goals are to better understand the behaviour of the test and to develop the exact success probabilities for the test against Clear *et al.*'s and Zhao *et al.*'s non-anonymized IBE schemes.

Let p and q be two primes and $n = pq$ be their product. In this section we will study the cardinalities of the following sets

$$\begin{aligned}
P_p^\ell(R) &= \{f_0x + f_1 \in \mathbb{Z}_p[x]/(x^2 - R) \mid J_p(f_1^2 - f_0^2R) = \ell\} \\
P_n^0(R) &= \{f_0x + f_1 \in \mathbb{Z}_n[x]/(x^2 - R) \mid J_n(f_1^2 - f_0^2R) = 0\} \\
P_n^{\ell_1,\ell_2}(R) &= \{f_0x + f_1 \in \mathbb{Z}_n[x]/(x^2 - R) \mid J_p(f_1^2 - f_0^2R) = \ell_1, J_q(f_1^2 - f_0^2R) = \ell_2\},
\end{aligned}$$

[5] since we are working with polynomials from $Z_n[x]/(x^2 - R)$ and not $Z_n^*[x]/(x^2 - R)$

where $\ell \in \{-1, 0, 1\}$ and $\ell_1, \ell_2 \in \{-1, 1\}$.

Before stating our results, we first present a lemma from [13] that further helps us compute our desired cardinalities.

Lemma 1 ([13]). *Let $p > 2$ be a prime, $k = p \operatorname{div} 4$, and $R \in \mathbb{Z}_p^*$. Then,*

$$|QR_p(a + QR_p)| = \begin{cases} k-1, & \textit{if } p = 4k+1 \textit{ and } R \in QR_p \\ k, & \textit{if } p = 4k+1 \textit{ and } R \in QNR_p, \textit{ or } p = 4k+3. \end{cases}$$

Now let us compute the cardinality of P_p^ℓ.

Lemma 2. *The following statements are true*

1. *If $R \in QNR_p$ then $|P_p^0(R)| = 1$, else $|P_p^0(R)| = 2p - 1$.*
2. *If $R \in QNR_p$ then $|P_p^1(R)| = (p^2 - 1)/2$, else $|P_p^1(R)| = (p-1)^2/2$.*
3. *If $R \in QNR_p$ then $|P_p^{-1}(R)| = (p^2 - 1)/2$, else $|P_p^{-1}(R)| = (p-1)^2/2$.*

Proof. To prove the first statement, we simply have to count the elements that satisfy $f_1^2 \equiv f_0^2 R \bmod p$. If $R \in QNR_p$, our single option is $f_0 = f_1 = 0$. Otherwise, for each non-zero value of f_0^2 we have two distinct f_1 values. Hence, we obtain $2(p-1)$ possibilities.

Now we will prove the second statement. When $f_0, f_1 \not\equiv 0 \bmod p$, we can rewrite $f_1^2 - f_0^2 R$ as $c^2 - R$, where $c \equiv f_0^{-1} f_1 \bmod p$. Using Lemma 1, we obtain that the number of possibilities is

$$\begin{cases} k-1, & \text{if } p = 4k+1 \text{ and } R \in QR_p \\ k, & \text{if } p = 4k+1 \text{ and } R \in QNR_p, \text{ or } p = 4k+3. \end{cases}$$

When $f_0 \equiv 0 \bmod p$, we obtain that $J_p(f_1^2) = 1$ and this is true only if $f_1 \not\equiv 0 \bmod p$. Hence, we obtain $p - 1$ possibilities.

In the case $f_1 \equiv 0 \bmod p$, we obtain that $J_p(-f_0^2 R) = 1$, and thus $f_0 \not\equiv 0 \bmod p$. When $-R \in QR_p$, we obtain $p-1$ possibilities and when $-R \in QNR_p$ we have none.

Adding all the possibilities we obtain

$$\begin{cases} (p-1)[(p-5)/2+2] = (p-1)^2/2 & \text{if } p = 4k+1 \text{ and } R \in QR_p \\ (p-1)[(p-1)/2+1] = (p^2-1)/2 & \text{if } p = 4k+1 \text{ and } R \in QNR_p \\ (p-1)[(p-3)/2+1] = (p-1)^2/2 & \text{if } p = 4k+3 \text{ and } R \in QR_p \\ (p-1)[(p-3)/2+2] = (p^2-1)/2 & \text{if } p = 4k+3 \text{ and } R \in QNR_p \end{cases}$$

The last statement is obtained by subtracting the cardinalities of $P_p^0(R)$ and $P_p^1(R)$ from $|\mathbb{Z}[x]/(x^2 - R)|$. □

Using the Chinese remainder theorem, we obtain the following cardinalities.

Corollary 1. *The following statements are true*

1. *If* $R \in J_n \setminus QR_n$ *then* $|P_n^0(R)| = p^2 + q^2 - 1$*, else* $|P_n^0(R)| = (2p-1)q^2 + (2q-1)(p-1)^2$.
2. *If* $R \in J_n \setminus QR_n$ *then* $|P_n^{\ell_1,\ell_2}(R)| = (p^2-1)(q^2-1)/4$*, else* $|P_n^{\ell_1,\ell_2}(R)| = (p-1)^2(q-1)^2/4$.

Let $h(x)$ be a polynomial such that $GT_n(R, h(x)) = -1$ and $A \subseteq \mathbb{Z}_n[x]/(x^2 - R)$ a set of polynomials. We further define the set

$$T_n(R, h(x), A) = \{h(x) \cdot f(x) \mid f(x) \in A\}.$$

Lemma 3. *The following identity holds* $|T_p(R, h(x), A)| = |A|$.

Proof. If $R \in QNR_p$ then the polynomial $x^2 - R$ is irreducible. Hence, $\mathbb{Z}_p[x]/(x^2 - R)$ is a field. Therefore, $h(x)$ only permutes the set A.

When $R \in QR_p$ we distinguish two case. When $h(x)^{-1}$ exists, then we again have a permutation of the set. Otherwise, $h(x)$ has the form $h(x) = t(x \pm r)$, for a $t \in \mathbb{Z}_p^*$. But in this case we obtain that $(tr)^2 - t^2R = 0$ and this contradicts our assumption ($i.e$ $GT_n(R, h(x)) = -1$). Hence, $h(x)^{-1}$ always exists. □

Corollary 2. *The following identity holds* $|T_n(R, h(x), A)| = |A|$.

We further present a lemma that states that the generalized Galbraith test is "multiplicative". This lemma stays at the base of the anonymization technique described in [6,7].

Lemma 4 ([6,7]). *Let* $e(x) \equiv f(x) \cdot g(x) \bmod x^2 - R$*. Then* $GT_n(R, e(x)) = GT_n(R, f(x)) \cdot GT_n(R, g(x))$.

4 Clear *et al.* IBE scheme

4.1 Scheme Description

Clear *et al.* [6] were the first to study the algebraic structure of Cocks' ciphertexts. A more in depth study of the underlying structure can be found in [9,10,13]. As a result of Clear *et al.*'s study, the authors managed to describe a partially homomorphic IBE scheme [6] and later they improve the scheme such that is also anonymous [7].

We further present a slightly improved version of Clear *et al.*'s IBE scheme. We start by presenting the non-anonymized version.

Setup(λ): Given a security parameter λ, generate two primes $p, q > 2^\lambda$ and compute their product $n = pq$. The public parameters are $pp = \{n, u, H, H'\}$ and the master secret key is $msk = \{p, q\}$, where $u \in \mathbb{Z}_n$ such that $J_p(u) = J_q(u) = -1$, $H : \{0,1\}^* \to J_n$ and $H' : \{0,1\}^* \to \mathbb{Z}_n(x)/(x^2 - R)$ are two cryptographic hash functions. Note that H' must also satisfy the property that for any identity $id \in \{0,1\}^*, R \leftarrow H(id)$ and $h(x) \leftarrow H'(id)$, it holds that

$$GT_n(R, h(x)) = GT_n(uR, h(x)) = -1.$$

KeyGen(pp, msk, id): Let $R = H(id)$. If $R \in QR_n$, then compute $r \equiv R^{1/2} \bmod n$. Otherwise, computes $r \equiv (uR)^{1/2} \bmod n$. The private key is r.

Enc(pp, id, m): On inputting pp, an identity id and a message $m \in \{-1, 1\}$, compute the hash value $R = H(id)$ and randomly choose two polynomials $f(x), \overline{f}(x)$ of degree 1 from $\mathbb{Z}_n[x]$ such that $J_n(f_1) = J_n(\overline{f}_1) = m$, where $f_1 = f(0)$ and $\overline{f}_1 = \overline{f}(0)$. Also, calculate

$$g(x) \equiv f_1^{-1} \cdot f(x)^2 \bmod (x^2 - R) \text{ and } \overline{g}(x) \equiv (\overline{f}_1)^{-1} \cdot \overline{f}(x)^2 \bmod (x^2 - uR).$$

Return the ciphertext $C = (g(x), \overline{g}(x))$.

Dec(r, C): On input pp, a secret key r and a ciphertext $C = (c(x), \overline{c}(x))$, compute

$$m' = \begin{cases} J_n(c(r)) & \text{if } r^2 \equiv H(id) \bmod n; \\ J_n(\overline{c}(r)) & \text{otherwise.} \end{cases}$$

Correctness : The correctness of the decryption algorithm follows by noticing that when $r^2 \equiv H(id) \bmod n$ we have

$$m' = J_n(c(r)) = J_n(f_1^{-1} \cdot f(r)^2) = J_n(f_1^{-1}) = m.$$

When $r^2 \equiv uH(id) \bmod n$, we can proceed similarly.

Using the generalized Galbraith test, it can be shown that the scheme is not anonymous (see Section 4.2). Hence, we need to upgrade the scheme with an anonymization algorithm. We further describe the method as presented in [6,7]. Note that the *Anon* algorithm anonymizes the ciphertext, while the *DeAnon* reverses the process.

Anon(pp, id, C): Given the public parameters pp, an identity id and a ciphertext $C = (c(x), \overline{c}(x))$, compute $R = H(id)$ and $h(x) = H'(id)$. Also, generate two random bits $v_1, v_2 \in \{0, 1\}$ and calculate

$$g(x) \equiv g(x) \cdot h(x)^{v_1} \bmod (x^2 - R)$$
$$\overline{g}(x) \equiv \overline{g}(x) \cdot h(x)^{v_2} \bmod (x^2 - uR).$$

Return the anonymized ciphertext $C' = (g(x), \overline{g}(x))$.

DeAnon(pp, id, C) On input pp, a secret key r and a ciphertext $C = (c(x), \overline{c}(x))$, compute $R = H(id)$, $h(x) = H'(id)$ and

$$g(x) \equiv g(x) \cdot h(x)^{(1-w_1)/2} \bmod (x^2 - R)$$
$$\overline{g}(x) \equiv \overline{g}(x) \cdot h(x)^{(1-w_2)/2} \bmod (x^2 - uR),$$

where $w_1 = GT_n(R, c(x))$ and $w_2 = GT_n(R, \overline{c}(x))$. Return the non-anonymized ciphertext $C' = (g(x), \overline{g}(x))$.

Previous Analysis. Let $f(x) = ax + b$, where $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_n^*$. Note that $J_n(b)$ is our message. Then

$$b^{-1} \cdot f(x)^2 \equiv b^{-1} \cdot (a^2R^2 + b^2 + 2abx) \equiv a^2b^{-1}R^2 + b + 2ax \bmod x^2 - R.$$

In the IBE scheme presented in [6], the authors select random polynomials $f(x)$ until $GT_n(R, f(x)) = 1$. Also, when proving the security of their scheme, they also impose an additional restriction, that $a^2b^{-1}R^2 + b \in \mathbb{Z}_n^*$. In the updated version of the scheme [7], the authors simply generate polynomials until $a^2b^{-1}R^2 + b \in \mathbb{Z}_n^*$. Using these restrictions, we can reduce the generalized version of Galbraith's test to the original version. But, in reality we should not be able to distinguish the polynomials generated by the IBE scheme from random polynomials from $\mathbb{Z}[x]/(x^2 - R)$. For this reason, in our version we removed the requirement $a^2b^{-1}R^2 + b \in \mathbb{Z}_n^*$ and as we shall see next we can prove that we cannot distinguish these polynomials from random ones.

4.2 New Analysis

We first study the cardinality of the set

$$D_n(R) = \{b^{-1}(ax + b)^2 \bmod x^2 - R \mid a \in \mathbb{Z}_n, b \in \mathbb{Z}_n^*\},$$

which contains the polynomials generated by the scheme presented in Section 4.1. Note that we further consider that $R \neq 0$. Otherwise, we can trivially recover b by computing $f(0)$.

Lemma 5. *If $R \in QNR_p$ then $|D_p(R)| = (p^2 - 1)/2$, otherwise $|D_p(R)| = (p-1)(p+3)/2$.*

Proof. Rewriting $b^{-1}(ax + b)^2 = d^{-1}(cx + d)^2$ we obtain

$$a^2dR + b^2d \equiv c^2bR + d^2b \bmod p$$
$$2abd \equiv 2cdb \bmod p.$$

From the second equation we obtain $a \equiv c \bmod p$. Keeping this in mind, the first equation becomes $(d - b)(a^2R - bd) \equiv 0 \bmod p$. If $a \equiv 0 \bmod p$, then we obtain that $d \equiv b \bmod p$ since $b, d \in \mathbb{Z}_p^*$. Else, either $d \equiv b \bmod p$ or $d \equiv b^{-1}a^2R \bmod p$.

We further consider $a \not\equiv 0 \bmod p$. If $R \in QNR_p$ then $b \not\equiv b^{-1}a^2R \bmod p$, otherwise from $b \equiv \pm aR^{1/2} \bmod p$ we obtain $b \equiv b^{-1}a^2R \bmod p$. Therefore, if $R \in QNR_p$ we obtain that $|D_p(R)| = (p-1)(p-1)/2 + p - 1 = (p-1)(p+1)/2$. Otherwise, we obtain $|D_p(R)| = [(p-3)/2 + 2](p-1) + p - 1 = (p-1)(p+3)/2$. □

Corollary 3. *If $R \in J_n \backslash QR_n$ then $|D_n(R)| = (p^2-1)(q^2-1)/4$ and if $R \in QR_n$ then $|D_n(R)| = (p-1)(p+3)(q-1)(q+3)/4$.*

Now, we consider the set of ciphertexts that can be correctly decrypted

$$D_n^*(R) = \{b^{-1}(ax + b)^2 \bmod x^2 - R \mid a \in \mathbb{Z}_n; b, ar + b \in \mathbb{Z}_n^*\}.$$

Lemma 6. *When $R \in QR_p$ we have $|D_p^*(R)| = (p^2-1)/2$.*

Proof. From $ar + b \equiv 0 \bmod p$ we obtain $a \equiv -br^{-1} \bmod p$ since $r, b \in \mathbb{Z}_n^*$. Looking at the proof of Lemma 5, we observe that in the case $a \equiv 0 \bmod p$ the sets are not affected by the added restriction since $-br^{-1} \not\equiv 0 \bmod p$. When $a \not\equiv 0 \bmod p$, the only case that is affected is $b \equiv -ar \bmod p$. Therefore, we obtain our desired result. □

Corollary 4. *If $R \in QR_n$ then $|D_n^*(R)| = (p^2-1)(q^2-1)/4$.*

Corollary 5. *The probability of correct decryption is $1 - \mathcal{O}(1/n)$.*

Proof. From Corollaries 3 and 4 we obtain that the probability is

$$\frac{|D_n^*(R)|}{|D_n(R)|} = \frac{(p+1)(q+1)}{(p+3)(q+3)} \simeq 1 - \mathcal{O}\left(\frac{1}{n}\right).$$

□

Now we will study ciphertexts with a given generalized Galbraith value. Thus, we define

$$D_p^\ell(R) = \{f_0x + f_1 \in D_p(R) \mid J_p(f_1^2 - f_0^2R) = \ell\}$$
$$D_n^0(R) = \{f_0x + f_1 \in D_n(R) \mid J_n(f_1^2 - f_0^2R) = 0\}$$
$$D_n^1(R) = \{f_0x + f_1 \in D_n(R) \mid J_p(f_1^2 - f_0^2R) = J_q(f_1^2 - f_0^2R) = 1\},$$

where $\ell \in \{0, 1\}$.

Lemma 7. *The following statements are true*

1. *If $R \in QNR_p$ then $|D_p^0(R)| = 0$, else $|D_p^0(R)| = 2(p-1)$.*
2. *If $R \in QNR_p$ then $|D_p^1(R)| = (p^2-1)/2$, else $|D_p^1(R)| = (p-1)^2/2$.*

Proof. Since $f \in D_p^0(R)$ we have $(a^2b^{-1}R + b)^2 - 4a^2R \equiv 0 \bmod p$. This is equivalent with $a^2b^{-1}R - b \equiv 0 \bmod p$. If $R \in QNR_p$, then $D_p^0(R) = \emptyset$. Otherwise, we obtain $(ar - b)(ar + b) \equiv 0 \bmod p$. Thus, we can rewrite the set as $D_p^0(R) = \{2ar(x \pm r) \mid a \in \mathbb{Z}_p^*\}$.

We further count the distinct elements of $D_p^0(R)$. From $2a(x \pm r) \equiv 2c(x \pm r) \bmod x^2 - R$ we obtain $a \equiv \pm c \bmod p$. From $2a(x+r) \equiv 2c(x-r) \bmod x^2 - R$ we obtain $a(x+r) + c(-x+r) \equiv 0 \bmod x^2 - R$. Hence, we obtain $a = c = 0$ which is impossible. Thus, the cardinality of $D_p^0(R)$ is $2(p-1)$.

The last statement results from observing that all the elements from $D_p(R)$ have the Jacobi symbol $J_p(f_1^2 - f_0^2R)$ either 1 or 0 when $R \in QR_p$. Hence, using Lemma 5 we obtain our result. □

Corollary 6. *The following statements are true*

1. *If $R \in J_n \setminus QR_n$ then $|D_n^0(R)| = 0$, else if $R \in QR_n$ $|D_n^0(R)| = (p-1)(q-1)(p+q+2)$.*

2. *If $R \in J_n \setminus QR_n$ then $|D_n^1(R)| = (p^2-1)(q^2-1)/4$, else if $R \in QR_n$ $|D_n^1(R)| = (p-1)^2(q-1)^2/4$.*

Now we can proper analyze the efficiency of the generalized Galbraith test.

Corollary 7. *The probability that a ciphertexts $f(x)$ produced by the scheme from Section 4.1 has $GT_n(R, f(x)) = 1$ is $1 - \mathcal{O}(1/n)$.*

Proof. According to Corollaries 4 and 6 we have

$$\frac{|D_n^1(R)|}{|D_n(R)|} = \begin{cases} 1 & \text{if } R \in J_n \setminus QR_n \\ \frac{(p+1)(q+1)}{(p+3)(q+3)} \simeq 1 + \mathcal{O}\left(\frac{1}{n}\right) & \text{if } R \in QR_n. \end{cases}$$

□

Corollary 8. *The generalized Galbraith test can detect ciphertexts produced by the scheme from Section 4.1 with a probability of $1/2 + \mathcal{O}(1/n)$.*

Proof. According to Corollaries 1 and 3 we have

$$\frac{|D_n(R)|}{|P_n^{1,1}(R) \cup P_n^{-1,-1}(R)|} = \begin{cases} 1/2 & \text{if } R \in J_n \setminus QR_n \\ \frac{(p+3)(q+3)}{2(p+1)(q+1)} \simeq \frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right) & \text{if } R \in QR_n. \end{cases}$$

□

Lemma 8. *The following equality holds $D_p^1(R) = P_p^{1,1}(R)$.*

Proof. We will show that $P_p^{1,1}(R) \subseteq D_p^1(R)$ and $D_p^1(R) \subseteq P_p^{1,1}(R)$. Our second inclusion is trivial because $P_p^{1,1}(R)$ contains all possible 1-degree polynomials which have Jacobi symbol equal to 1. Now, let us focus on the first inclusion. We take a random $f = f_0x + f_1 \in P_p^{1,1}(R)$ and we search for a pair $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p^*$ such that $f_0x + f_1 = b^{-1}(ax + b)^2 = 2ax + a^2Rb^{-1} + b$. From this we have $f_0 \equiv 2a \bmod p$ and $f_1 \equiv a^2Rb^{-1} + b \bmod p$. As a result, we can derive $a \equiv 2^{-1}f_0 \bmod p$ and $b^2 - bf_1 + 4^{-1}f_0^2R \equiv 0 \bmod p$. Therefore, we obtain $\Delta = f_1^2 - 4 \cdot 4^{-1}f_0^2R = f_1^2 - f_0^2R$ which has the Jacobi symbol 1 according to the definition of $P_p^{1,1}(R)$.

Now let us assume that $b \equiv 0 \bmod p$. Then we have $f_1 \pm (f_1^2 - f_0^2R)^{1/2} \equiv 0 \bmod p$. This implies that $f_0^2R \equiv 0 \bmod p$. Since, $R \not\equiv 0 \bmod p$ we obtain that $f_0 \equiv 0 \bmod p$ and implicitly $a \equiv 0 \bmod p$. But, when $a \equiv 0 \bmod p$ we can choose the other root $b \equiv f_1 \bmod p$, which is different from 0 since we cannot have both f_0 and f_1 equal to 0.

When $f_0 \not\equiv 0 \bmod p$, we can choose b as either of the two roots[6]. Thus, we obtain that $f \in D_p^1(R)$. This concludes our proof. □

Corollary 9. *The following equality holds $D_n^1(R) = P_n^{1,1}(R)$.*

Corollary 10. *Either $T_n(R, h(x), D_n^1(R)) = P_n^{1,-1}(R)$ or $T_n(R, h(x), D_n^1(R)) = P_n^{-1,1}(R)$ depending if either $GT_p(R, h(x)) = 1$ or $GT_q(R, h(x)) = 1$.*

[6] $\Delta \not\equiv 0 \bmod p$

Proof. We assume without loss of generality that $GT_p(R, h(x)) = 1$. Using Corollary 9 we obtain the following equality $T_n(R, h(x), D_n^1(R)) = T_n(R, h(x), P_n^{1,1}(R))$. Since $P_n^{1,-1}(R)$ contains all the polynomials $f(x)$ with $GT_n(R, f(x)) = -1$ and the generalized Galbraith test is "multiplicative" (see Lemma 4), we have $T_n(R, h(x), P_n^{1,1}(R)) \subseteq P_n^{1,-1}(R)$.

For the second inclusion we use the fact that $h(x)$ has an inverse (see the proof of Lemma 3). Hence, $T_n(R, h(x)^{-1}, P_n^{1,-1}(R)) \subseteq P_n^{1,1}(R)$. This relation can be rewritten as $P_n^{1,-1}(R) \subseteq T_n(R, h(x), P_n^{1,1}(R))$. This concludes our proof. □

Remark 1. Corollary 10 is also proven in [7], but using different techniques. We chose to reprove it since it follows directly from our analysis.

We further assume without loss of generality that $GT_p(R, h(x)) = 1$.

Corollary 11. *Let* $P_n^{+,-}(R) = P_n^{1,1}(R) \cup P_n^{1,-1}(R)$ *and* $\tilde{D}_n(R) = D_n^1(R) \cup T_n(R, h(x), D_n^1(R))$. *Then the distributions*

$$X_n = \{f(x) \mid f(x) \xleftarrow{\$} \tilde{D}_n(R)\}$$
$$Y_n = \{f(x) \mid f(x) \xleftarrow{\$} P_n^{+,-}(R)\}$$

are identical.

In order to prove that their anonymization technique is secure, Clear *et al.* first established a series of computational indistinguishability results. The one that we are interested in states that

$$Z_n = \{GT_n(R, f(x)) \mid f(x) \xleftarrow{\$} \tilde{D}_n(R)\}$$

is computationally indistinguishable from the uniform distribution U on $\{-1, 1\}$, under the QR assumption. In [13], the authors prove a stronger result: the two distributions are statistically indistinguishable. Since we removed Clear *et al.*'s restriction, we need to prove that the statistically indistinguishability still holds. Using the results developed in this subsection we can prove exactly that.

Theorem 1. *The following distribution*

$$Z_n = \{GT_n(R, f(x)) \mid f(x) \xleftarrow{\$} \tilde{D}_n(R)\}$$

is statistically indistinguishable from the uniform distribution U *on* $\{-1, 1\}$.

Proof. We will show that the statistical distance $\Delta(Z_n, U)$ between Z_n and U is negligible, where

$$\Delta(Z_n, U) = \frac{1}{2} \sum_{b \in \{-1,1\}} \mid Pr[Z_n = b] - Pr[U = b] \mid .$$

Let $\overline{D}_n(R) = T_n(R, h(x), D_n(R))$ and $\overline{D}^1_n(R) = T_n(R, h(x), D^1_n(R))$. In order to compute $Pr[Z_n = b]$ we make use of Corollaries 1 and 2. Thus, taking into account that

$$Pr[f(x) \in D_n(R)] = Pr[f(x) \in \overline{D}_n(R)] = 1/2,$$

and that $f(x) \xleftarrow{\$} D_n(R) \cup \overline{D}_n(R)$, we obtain

$$\begin{aligned} Pr[Z_n = 1] &= Pr[GT_n(R, f(x)) = 1] \\ &= Pr[GT_n(R, f(x)) = 1 \mid f(x) \in D_n(R)] \cdot Pr[f(x) \in D_n(R)] \\ &+ Pr[GT_n(R, f(x)) = 1 \mid f(x) \in \overline{D}_n(R)] \cdot Pr[f(x) \in \overline{D}_n(R)] \\ &= \frac{1}{2} \cdot \frac{|D^1_n(R)|}{|\tilde{D}_n(R)|} + \frac{1}{2} \cdot \frac{|\overline{D}^1_n(R)|}{|\tilde{D}_n(R)|} = \frac{|D^1_n(R)|}{|\tilde{D}_n(R)|} \\ &= \frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right). \end{aligned}$$

In a similar way one can obtain

$$Pr[Z_n = -1] = \frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right).$$

Now, the statistical distance $\Delta(Z_n, U)$ becomes

$$\Delta(X_n, U) = \frac{1}{2}\left(\left|\frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right) - \frac{1}{2}\right| + \left|\frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right) - \frac{1}{2}\right|\right) = \mathcal{O}\left(\frac{1}{n}\right).$$

Since n is exponentially large in the security parameter λ, the statistical distance is negligible. □

5 Zhao *et al.* IBE scheme

5.1 Scheme Description

In [15], the authors introduce two IBE schemes that work with polynomials modulo n, where n is the product of two primes p, q chosen such that $p \equiv -q \bmod 4$. Zhao *et al.* prove the security of their schemes under the strong QR assumption[7].

Starting from their first scheme, we devised a new scheme from which we removed the necessity of choosing $p \equiv -q \bmod 4$. In this case, the proof from [15] can be easily adapted to obtain that our scheme is secure under the QR assumption.

Setup(λ): Given a security parameter λ, generate two primes $p, q > 2^\lambda$ and compute their product $n = pq$. Randomly generate two integers $u, y \in \mathbb{Z}$ such that $J_p(u) = J_q(u) = -1$ and $J_p(y) = -J_q(y)$. The public parameters are $pp = \{n, u, y, H\}$, where $H : \{0,1\}^* \to J_n$ is a cryptographic hash function. The master secret key is $msk = \{p, q\}$.

[7] which is basically the QR assumption with the restriction that $p \equiv -q \bmod 4$

KeyGen(pp, msk, id): Let $R = H(id)$. If $R \in QR_n$, then compute $r \equiv R^{1/2} \bmod n$. Otherwise, computes $r = (uR)^{1/2} \bmod n$. The private key is r.

Enc(pp, id, m): On inputting pp, an identity id and a message $m \in \{0, 1\}$, compute the hash value $R = H(id)$ and randomly chooses two polynomials $f(x), \overline{f}(x)$ of degree 1 from $\mathbb{Z}_n[x]$. Also, calculate

$$g(x) = f(x)^2 \bmod (x^2 - R) \quad \text{ and } \quad \overline{g}(x) = \overline{f}(x)^2 \bmod (x^2 - uR).$$

Return the ciphertext $C = (y^m \cdot g(x), y^m \cdot \overline{g}(x))$.

Dec(pp, r, C): On input pp, a secret key r and a ciphertext $C = (c(x), \overline{c}(x))$, compute

$$m' = \begin{cases} J_n(c(r)) & \text{if } r^2 \equiv H(id) \bmod n; \\ J_n(\overline{c}(r)) & \text{otherwise.} \end{cases}$$

Correctness : The correctness of the decryption algorithm follows by noticing that when $r^2 \equiv H(id) \bmod n$ we have

$$m' = J_n(c(r)) = J_n(y^m \cdot f(r)^2) = [J_p(y) \cdot J_q(y)]^m = [-J_p(y)^2]^m = (-1)^m,$$

and thus we can recover the message m. When $r^2 \equiv uH(id) \bmod n$, we can proceed similarly.

Although this proposal is not anonymous (see Section 5.2), it can be made as such by using the same anonymization technique as in Section 4.1.

Previous Work. When $p \equiv -q \bmod 4$ and $y = -1$ we obtain the scheme described in [15]. Note that in this case we can choose $h(x) = x$ since $GT_n(R, x \cdot c(x)) = -GT_n(R, c(x))$. When analyzing the scheme, the authors do not prove the success probability of decryption and of the generalized Galbraith test against their first proposal. Also, when computing the size of the ciphertext space, Zhao *et al.* managed to prove that it is at least $(p-1)(p-3)(q-1)(q-3)/16$ (see the next section for the exact size). Two other aspects that are not rigorously stated are: the two complexity assumptions used to prove the anonymity of their second scheme and their argument that leads to the necessity of these two assumptions.

5.2 New Analysis

We start with studying the cardinality of the following sets

$$C_{n,0}(R) = \{(ax + b)^2 \bmod x^2 - R \mid a, b \in \mathbb{Z}_n\},$$
$$C_{n,1}(R) = \{y(ax + b)^2 \bmod x^2 - R \mid a, b \in \mathbb{Z}_n\},$$

which contain the polynomials generated by the scheme presented in Section 5.1. Note that we further consider that $R \neq 0$. Otherwise, we can trivially recover m by computing $J_n(g(0)) = J_n(y^m b^2) = J_n(y^m) = (-1)^m$.

Lemma 9. *Let $R \in QR_p$. If $J_p(y) = -1$ then $C_{p,0}(R) \cap C_{p,1}(R) = \{0\}$, else we have $C_{p,0}(R) = C_{p,1}(R)$. We also have $|C_{p,0}(R)| = |C_{p,1}(R)| = (p+1)^2/4$.*

Proof. Let $J_p(y) = -1$. We first prove that the sets $C_{p,0}(R) \cap C_{p,1}(R) = \{0\}$. Let $f(x) \in C_{p,0}(R) \cap C_{p,1}(R)$. Then $f(x) \equiv (ax+b)^2 \bmod x^2 - R$ and $f(x) \equiv y(cx+d)^2 \bmod x^2 - R$ for $a, b, c, d \in \mathbb{Z}_p$. This is identical with

$$\begin{aligned} a^2R + b^2 &\equiv y(c^2R + d^2) \bmod p \\ 2ab &\equiv 2cdy \bmod p \end{aligned}$$

which is equivalent with

$$\begin{aligned} (ar+b)^2 &\equiv y(cr+d)^2 \bmod p \\ (ar-b)^2 &\equiv y(cr-d)^2 \bmod p. \end{aligned}$$

If $a, b, c, d \neq 0$, from any of the equations we obtain that $y \in QR_p$. Therefore, we obtain a contradiction, and thus $a = b = c = d = 0$.

When $J_p(y) = 1$, we have

$$f(x) \equiv y(ax+b)^2 \equiv u^2(ax+b)^2 \equiv (uax+ub)^2 \bmod x^2 - R,$$

where $u^2 \equiv y \bmod p$. Hence, if $f(x) \in C_{p,1}(R)$ then $f(x) \in C_{p,0}(R)$. Similarly, we obtain that $f(x) \in C_{p,0}(R)$ then $f(x) \in C_{p,1}(R)$. Therefore, $C_{p,0}(R) = C_{p,1}(R)$.

Let $f_1(x) = (a_1x+b_1)^2, f_2(x) = (a_2x+b_2)^2 \in C_{p,0}(R)$. If $f_1(x) \equiv f_2(x) \bmod x^2 - R$, then $f_1(x)^{1/2} \equiv \pm f_2(x)^{1/2} \bmod x^2 - R$. Thus, $(a_1 \mp a_2)x + (b_1 \mp b_2) \equiv 0 \bmod x^2 - R$. Therefore, we have $a_1 \equiv \pm a_2 \bmod p$ and $b_1 \equiv \pm b_2 \bmod p$. Note that for $a_1 \neq 0$ we always have $a_1 \not\equiv -a_1 \bmod p$, and thus we obtain two numbers that reach the same value when squared. Similarly for b_1. Hence, we obtain that $|C_{p,0}(R)| = [(p-1)/2 + 1]^2 = (p+1)^2/4$. Similarly, we obtain $|C_{p,1}(R)| = (p+1)^2/4$. □

Corollary 12. *Let $R \in QR_n$. We assume without loss of generality that $J_p(y) = 1$. Then $|C_{n,0}(R)| = |C_{n,1}(R)| = (p+1)^2(q+1)^2/16$. Also, $|C_{n,0}(R) \cap C_{n,1}(R)| = (p+1)^2/4$ and $|C_{n,0}(R) \cup C_{n,1}(R)| = (p+1)^2(q+1)^2/8 - (p+1)^2/4$.*

Lemma 10. *Let $R \in QNR_p$. Then we have $|C_{p,0}(R)| = (p^2+1)/2$ and $C_{p,0}(R) = C_{p,1}(R)$.*

Proof. Since $R \in QNR_p$ then $\mathbb{Z}[x]/(x^2 - R)$ is a field. Let $f_1(x) = (a_1x + b_1)^2 \neq 0, f_2(x) = (a_2x+b_2)^2 \neq 0 \in C_{p,0}(R)$. If $f_1(x) \equiv f_2(x) \bmod x^2 - R$, then $(f_1(x)f_2(x)^{-1})^2 \equiv 1 \bmod x^2 - R$. Thus, $f_1(x)f_2(x)^{-1} \equiv \pm 1 \bmod x^2 - R$, which is equivalent with $f_1(x) \equiv \pm f_2(x) \bmod x^2 - R$. Hence, $|C_{p,0}(R)| = (p^2+1)/2$.

Let $f(x) \in C_{p,0}(R) \cap C_{p,1}(R)$. Then $f(x) \equiv g(x)^2 \bmod x^2 - R$ and $f(x) \equiv yh(x)^2 \bmod x^2 - R$ for $g(x), h(x) \in \mathbb{Z}_p[x]/(x^2 - R) \setminus \{0\}$. This is equivalent with

$$y \equiv (g(x)h(x)^{-1})^2 \equiv (v + wx)^2 \equiv v^2 + w^2R + 2vwx \bmod x^2 - R$$

which translates into

$$\begin{aligned} v^2 + w^2 R &\equiv y \bmod p \\ 2vwx &\equiv 0 \bmod p \end{aligned}$$

We either have $v = 0$ or $w = 0$. Hence, either $w^2 \equiv yR^{-1} \bmod p$ or $v^2 \equiv y \bmod p$. If $J_p(y) = -1$ then the second equality lead to a contradiction and hence $v = 0$ and $w \equiv (yR^{-1})^{1/2} \bmod p$. This leads to $g(x)h(x)^{-1} \equiv (yR^{-1})^{1/2} x \bmod x^2 - R$. Hence, we obtain that $C_{p,0}(R) = C_{p,1}(R)$. If $J_p(y) = 1$ then the first equality lead to a contradiction, and thus $v \equiv y^{1/2} \bmod p$ and $w = 0$. This leads to $g(x)h(x)^{-1} \equiv y^{1/2} \bmod x^2 - R$. Therefore, we obtain our desired result. □

Corollary 13. *Let $R \in J_n \setminus QR_n$. Then $C_{n,0}(R) = C_{n,1}(R)$ and $|C_{n,0}(R)| = (p^2 + 1)(q^2 + 1)/4$.*

Now, we consider the sets of ciphertexts that can be correctly decrypted

$$\begin{aligned} C^*_{n,0}(R) &= \{(ax + b)^2 \bmod x^2 - R \mid a, b \in \mathbb{Z}_n; ar + b \in \mathbb{Z}^*_n\}, \\ C^*_{n,1}(R) &= \{y(ax + b)^2 \bmod x^2 - R \mid a, b \in \mathbb{Z}_n; ar + b \in \mathbb{Z}^*_n\}. \end{aligned}$$

Lemma 11. *Let $R \in QR_p$. If $J_p(y) = -1$ then $C^*_{p,0}(R) \cap C^*_{p,1}(R) = \emptyset$, else we have $C^*_{p,0}(R) = C^*_{p,1}(R)$. We also have $|C^*_{p,0}(R)| = |C^*_{p,1}(R)| = (p^2 - 1)/4$.*

Proof. We first note that if $a = b = 0$, then $ax + b \notin \mathbb{Z}^*_n$. Using Lemma 9 we obtain the first statement.

Now, we want to see how many of these pairs are collapsing to the same polynomial value. Similarly to the proof of Lemma 9, from $f_1(x) \equiv f_2(x) \bmod x^2 - R$ we obtain $a_1 \equiv \pm a_2 \bmod p$ and $b_1 \equiv \pm b_2 \bmod p$. These numbers must also satisfy the restriction $b_1 \not\equiv -a_1 r \bmod p$.

We first consider the case $a_1 = a_2 = 0$. Since we have $b_1 \equiv a_1 r + b_1 \in \mathbb{Z}^*_p$, then there are $(p-1)/2$ non-collapsing values for b_1. On the other hand, if $a_1 \neq 0$, then for a_1 are able to find $(p-1)/2$ different non-collapsing values and for b_1 we are able to find $2 + (p-3)/2 = (p+1)/2$ non-collapsing values[8]. Hence, there will be $(p-1)(p+1)/4$ such polynomials in $C^*_{p,0}(R)$. Similarly, we obtain that $|C^*_{p,1}(R)| = (p^2 - 1)/4$. □

Corollary 14. *Let $R \in QR_n$. Then $|C^*_{n,0}(R)| = |C^*_{n,1}(R)| = (p^2-1)(q^2-1)/16$. Also, $C^*_{n,0}(R) \cap C^*_{n,1}(R) = \emptyset$ and $|C^*_{n,0}(R) \cup C^*_{n,1}(R)| = (p^2 - 1)(q^2 - 1)/8$.*

Corollary 15. *The probability of correct decryption is $1 + \mathcal{O}(1/n^2)$.*

Proof. From Corollaries 12 and 14 we obtain that the probability is

$$\frac{|C^*_{n,0}(R) \cup C^*_{n,1}(R)|}{|C_{n,0}(R) \cup C_{n,1}(R)|} = \frac{(p^2 - 1)(q^2 - 1)}{(p + 1)^2(q + 1)^2 - 8\delta} \simeq 1 + \mathcal{O}\left(\frac{1}{n^2}\right),$$

where $\delta \in \{(p + 1)^2/4, (q + 1)^2/4\}$. □

[8] We have to count the pairs $(a_1, 0)$ and $(a_1, a_1 r)$.

Now we will study ciphertexts with a given generalized Galbraith value. Thus, we define

$$\begin{aligned}
C_p^\ell(R) &= \{f_0x + f_1 \in C_{p,0}(R) \cup C_{p,1}(R) \mid J_p(f_1^2 - f_0^2R) = \ell\},\\
C_n^0(R) &= \{f_0x + f_1 \in C_{n,0}(R) \cup C_{n,1}(R) \mid J_n(f_1^2 - f_0^2R) = 0\},\\
C_n^1(R) &= \{f_0x + f_1 \in C_{n,0}(R) \cup C_{n,1}(R) \mid J_p(f_1^2 - f_0^2R) = J_q(f_1^2 - f_0^2R) = \ell\},
\end{aligned}$$

where $\ell \in \{0, 1\}$.

Lemma 12. *The following statements are true*

1. *If $R \in QNR_p$ then $|C_p^0(R)| = 1$, else*

$$|C_p^0(R)| = \begin{cases} p & \text{if } J_p(y) = 1,\\ 2p - 1 & \text{if } J_p(y) = -1. \end{cases}$$

2. *If $R \in QNR_p$ then $|C_p^1(R)| = (p^2 - 1)/2$, else*

$$|C_p^1(R)| = \begin{cases} (p-1)^2/4 & \text{if } J_p(y) = 1,\\ (p-1)^2/2 & \text{if } J_p(y) = -1. \end{cases}$$

Proof. Let $f = y^m(ax + b)^2 = y^m(a^2R + b^2 + 2abx)$, where $m \in \{0, 1\}$. We observe that $J_n(f_1^2 - f_0^2R) = J_n((a^2R + b^2)^2 - 4a^2b^2R)$. Hence, the Jacobi symbol is independent of y.

Since $f \in C_p^0(R)$ we have $(a^2R+b^2)^2 - 4a^2b^2R \equiv 0 \bmod p$. This is equivalent with $a^2R - b^2 \equiv 0 \bmod p$. If $R \in QNR_p$, then $C_p^0(R) = \{0\}$. Otherwise, we obtain $(ar - b)(ar + b) \equiv 0 \bmod p$. Thus, we can rewrite the set as $C_p^0(R) = \{2a^2ry^m(\pm x + r) \mid a \in \mathbb{Z}_p; m \in \{0, 1\}\}$. Let

$$\begin{aligned}
C_{p,0}^0(R) &= \{2a^2r(\pm x + r) \mid a \in \mathbb{Z}_p\},\\
C_{p,1}^0(R) &= \{2a^2ry(\pm x + r) \mid a \in \mathbb{Z}_p\}.
\end{aligned}$$

We further count the distinct elements of $C_{p,0}^0(R)$. From $2a^2r(\pm x + r) \equiv 2c^2r(\pm x + r) \bmod x^2 - R$ we obtain $a \equiv \pm c \bmod p$. From the relation $2a^2r(x + r) \equiv 2c^2r(-x + r) \bmod x^2 - R$ we obtain $a^2(x + r) + c^2(x - r) \equiv 0 \bmod x^2 - R$. Hence, we obtain $a = c = 0$. Thus, the cardinality of $C_{p,1}^0(R)$ is p.

Now let us consider the intersection of $C_{p,0}^0(R)$ and $C_{p,1}^0(R)$. From $2a^2r(\pm x + r) \equiv 2yc^2r(\pm x + r) \bmod x^2 - R$ we obtain $a \equiv \pm yc \bmod p$ if $J_p(y) = 1$ and $a = c = 0$ otherwise. Hence, $C_{p,0}^0(R) = C_{p,1}^0(R)$, if $J_p(y) = 1$ and $C_{p,0}^0(R) \cap C_{p,1}^0(R) = \{0\}$ otherwise.

The last statement results from observing that all the elements from $C_{p,0}(R) \cup C_{p,1}(R)$ have the Jacobi symbol $J_p(f_1^2 - f_0^2R)$ either 1 or 0. Hence, using Lemma 9 we obtain our result. □

Corollary 16. *We assume without loss of generality that $J_p(y) = 1$. Then the following statements are true*

1. *If* $R \in J_n \setminus QR_n$ *then* $|C_n^0(R)| = (p^2+q^2)/2$*, else if* $R \in QR_n$ $|C_n^0(R)| = (pq+1)(p+q)/2 - (p+1)^2/4$.
2. *If* $R \in J_n \setminus QR_n$ *then* $|C_n^1(R)| = (p^2-1)(q^2-1)/4$*, else if* $R \in QR_n$ $|C_n^1(R)| = (p-1)^2(q-1)^2/8$.

Corollary 17. *The probability that a ciphertexts* $f(x)$ *produced by the scheme from Section 5.1 has* $GT_n(R, f(x)) = 1$ *is* $1 + \mathcal{O}(1/n^2)$*.*

Proof. According to Corollaries 12, 13 and 16 we have

$$\frac{|C_n^1(R)|}{|C_{n,0}(R) \cup C_{n,1}(R)|} = \begin{cases} \frac{(p^2-1)(q^2-1)}{(p^2+1)(q^2+1)} \simeq 1 + \mathcal{O}\left(\frac{1}{n^2}\right) & \text{if } R \in J_n \setminus QR_n \\ \frac{(p-1)^2(q-1)^2}{(p+1)^2(q+1)^2 - 8\delta} \simeq 1 + \mathcal{O}\left(\frac{1}{n^2}\right) & \text{if } R \in QR_n, \end{cases}$$

where $\delta \in \{(p+1)^2/4, (q+1)^2/4\}$. □

Corollary 18. *The generalized Galbraith test can detect ciphertexts produced by the scheme from Section 5.1 with a probability of* $1/2 + \mathcal{O}(1/n^2)$ *if* $R \in J_n \setminus QR_n$ *and* $1/4 + \mathcal{O}(1/n^2)$ *if* $R \in QR_n$*.*

Proof. According to Corollaries 1, 12 and 13 we have

$$\frac{|C_n(R)|}{|P_n^{1,1}(R) \cup P_n^{-1,-1}(R)|} = \begin{cases} \frac{(p^2+1)(q^2+1)}{2(p^2-1)(q^2-1)} \simeq \frac{1}{2} + \mathcal{O}\left(\frac{1}{n^2}\right) & \text{if } R \in J_n \setminus QR_n \\ \frac{(p+1)^2(q+1)^2 - 8\delta}{4(p-1)^2(q-1)^2} \simeq \frac{1}{4} + O\left(\frac{1}{n^2}\right) & \text{if } R \in QR_n, \end{cases}$$

where $\delta \in \{(p+1)^2/4, (q+1)^2/4\}$. □

Using our results, we further redo the analysis from [15] and present the exact assumptions used to prove that the IBE scheme from Section 5.1 can be anonymized using the technique described in Section 4.1.

Let $P_n^+(R) = P_n^{1,1}(R) \cup P_n^{-1,-1}(R)$ and $C_n(R) = C_{n,0}(R) \cup C_{n,1}(R)$. According to Corollaries 1, 12 and 13 we have that $|P_n^+(R) \times P_n^+(uR)| = \mathcal{O}(p^2q^2)$ and $|C_n(R) \times C_n(uR)| = \mathcal{O}(3p^2q^2/8 - \delta)$, where $\delta \in \{p^2/4, q^2/4\}$. Since p and q are large primes we can make the following computational assumption

Assumption 1. For an identity id, the set $P_n^+(R) \times P_n^+(uR)$ is computationally indistinguishable from the ciphertext space when $v_1 = v_2 = 0$ (*i.e.* $C_n(R) \times C_n(uR)$).

Let $P_n^-(R) = P_n^{1,-1}(R) \cup P_n^{-1,1}(R)$. According to Corollaries 1, 2, 12 and 13 we have that $|P_n^-(R) \times P_n^-(uR)| = \mathcal{O}(p^2q^2)$ and

$$\begin{aligned} |T_n(R, h(x), C_n(R)) \times T_n(uR, h(x), C_n(uR))| &= |C_n(R) \times C_n(uR)| \\ &= \mathcal{O}(3p^2q^2/8 - \delta), \end{aligned}$$

where $\delta \in \{p^2/4, q^2/4\}$. Since p and q are large primes we can make the following computational assumption

Assumption 2. For an identity id, the set $P_n^+(R) \times P_n^-(uR)$ is computationally indistinguishable from the ciphertext space when $v_1 = v_2 = 1$ (*i.e.* $T_n(R, h(x), C_n(R)) \times T_n(uR, h(x), C_n(uR))$).

6 Conclusions

In this paper we reevaluate the extension of Galbraith's test to the polynomial ring $\mathbb{Z}_n[x]/(x^2 - R)$. By studying its exact behaviour, we were able to perform a deeper and a more rigorous analysis of Clear *et al.* and Zhao *et al.* IBE schemes. Therefore, we offer the reader a better understanding of these two schemes. To be more specific, we obtained a precise value for the probability of a successful decryption, the exact efficiency of the generalized Galbraith test and, in the case of Zhao *et al.* IBE scheme, a thorough description of the underlying security assumptions.

Future Work. In [14], the authors introduce an analog of Galbraith's test for higher residues. We believe that a more in depth study of this test can lead to a simpler description of it and can also help researchers to devise an anonymizing technique that renders this test ineffective.

References

1. Ateniese, G., Gasti, P.: Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In: CT-RSA 2009. Lecture Notes in Computer Science, vol. 5473, pp. 32–47. Springer (2009)
2. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-Privacy in Public-Key Encryption. In: ASIACRYPT 2001. Lecture Notes in Computer Science, vol. 2248, pp. 566–582. Springer (2001)
3. Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public Key Encryption with Keyword Search. In: EUROCRYPT 2004. Lecture Notes in Computer Science, vol. 3027, pp. 506–522. Springer (2004)
4. Boneh, D., Franklin, M.K.: Identity-Based Encryption from the Weil Pairing. In: CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 213–229. Springer (2001)
5. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: FOCS 2007. pp. 647–657. IEEE Computer Society (2007)
6. Clear, M., Hughes, A., Tewari, H.: Homomorphic Encryption with Access Policies: Characterization and New Constructions. In: AFRICACRYPT 2013. Lecture Notes in Computer Science, vol. 7918, pp. 61–87. Springer (2013)
7. Clear, M., Tewari, H., McGoldrick, C.: Anonymous IBE from Quadratic Residuosity with Improved Performance. In: AFRICACRYPT 2014. Lecture Notes in Computer Science, vol. 8469, pp. 377–397. Springer (2014)
8. Cocks, C.: An Identity Based Encryption Scheme Based on Quadratic Residues. In: IMACC 2001. Lecture Notes in Computer Science, vol. 2260, pp. 360–363. Springer (2001)
9. Joye, M.: Identity-Based Cryptosystems and Quadratic Residuosity. In: PKC 2016. Lecture Notes in Computer Science, vol. 9614, pp. 225–254. Springer (2016)
10. Nica, A.M., Țiplea, F.L.: On Anonymization of Cocks' Identity-based Encryption Scheme. Computer Science Journal of Moldova **81**(3), 283–298 (2019)
11. Schipor, G.A.: On the Anonymization of Cocks IBE Scheme. In: BalkanCryptSec 2014. Lecture Notes in Computer Science, vol. 9024, pp. 194–202. Springer (2014)

12. Shamir, A.: Identity-based cryptosystems and signature schemes. In: CRYPTO 1984. Lecture Notes in Computer Science, vol. 196, pp. 47–53. Springer (1985)
13. Ţiplea, F.L., Iftene, S., Teşeleanu, G., Nica, A.M.: On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography. Applied Mathematics and Computation **372**, 124993–124990 (2020)
14. Zhao, X., Cao, Z., Dong, X., Shao, J.: Extended Galbraith's Test on the Anonymity of IBE Schemes from Higher Residuosity. Des. Codes Cryptogr. **89**(2), 241–253 (2021)
15. Zhao, X., Cao, Z., Dong, X., Zheng, J.: Anonymous IBE from Quadratic Residuosity with Fast Encryption. In: ISC 2020. Lecture Notes in Computer Science, vol. 12472, pp. 3–19. Springer (2020)